CLAIMS

1. A method of generating successive round keys of an expanded key from an initial cryptographic key for use in an encryption and/or decryption engine, comprising the steps of:

storing the Nk words of the initial key in Nk locations of a memory;

providing the initial key to a cryptographic engine for performing a first cryptographic round;

repeatedly retrieving a selected first word and a selected second word of the expanded key, at least one of which is retrieved from the memory, and generating from the selected first and second words a successive subsequent word of the expanded key;

providing the generated words of the expanded key to the cryptographic engine as round keys for performing subsequent cryptographic rounds; and

storing successive ones of the generated subsequent words in the memory by cyclically overwriting previously generated words of the expanded key.

2. The method of claim 1 in which the step of overwriting previously generated words only occurs after those words have been used as said first and/or said second selected words in the step of generating a respective subsequent word.

3. The method of claim 1 in which the number of memory locations used is less than the number of words in the expanded key.

4. The method of claim 1 in which the number of memory locations used is equal to Nk.

5. The method of claim 4 in which the words of the initial key are also overwritten by words of the expanded key during the overwriting step.

6. The method of claim 1 in which the number of memory locations used is equal to 2Nk.

7. The method of claim 1 in which the memory is divided into two parts, a first part storing the initial key and the second part receiving the successively generated words of the expanded key.

8. The method of claim 7 further including the step of completing generation of the expanded key such that the final round key is stored in the second part of the memory and the initial key is still stored in the first part of the memory.

9. The method of claim 8 further including the step of performing a repeat key expansion starting with the initial key stored in the first part of the memory.

10. The method of claim 8 further including the step of performing an inverse key expansion starting with the final round key stored in the second part of the memory.

11. The method of any one of claims 1 to 4 further including the step of completing generation of the expanded key such that the final round key is stored in the memory and the initial key has been overwritten.

12. The method of claim 11 further including the step of performing an inverse key expansion starting with the final round key stored in the memory in order to regenerate the initial key for a subsequent cryptographic operation.

13. The method of claim 7 in which the number of memory locations used is equal to 2Nk, the first and the second parts having Nk locations each.

14. The method of any preceding claim in which the step of generating successive subsequent words of the expanded key comprises generating successive words of the AES Rijndael block cipher round keys according to the AES key expansion function.

15. The method of claim 14 in which Nk = 8.

16. The method of any preceding claim in which the successive subsequent words of the expanded key comprise words of encryption round keys.

17. The method of any one of claims 1 to 15 in which the successive subsequent words of the expanded key comprise words of decryption round keys.

18. The method of claim 1 in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing the words on a word-by-word basis as the cryptographic engine consumes the words as round keys.

19. The method of claim 1 in which, in the retrieving step, both the selected first word and the selected second word are retrieved from the memory.

20. The method of claim 1 in which, in the retrieving step, the selected first word is retrieved from memory and the selected second word is retrieved from a register used in a previous iteration.

21. The method of claim 1 in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing said generated words from the memory.

22. The method of claim 1 in which the step of generating includes, in at least some cycles of round key word generation, the step of performing an S-box transform using an S-box shared with the cryptographic engine.

23. The method of claim 22 further including the step of maintaining synchronism of the generation of successive round key words with consumption of the round key words by the cryptographic engine.

24. A round key generator for generating successive round keys of an expanded key from an initial cryptographic key for use in an encryption and/or decryption engine, comprising:

a memory for storing the Nk words of the initial key;

an expansion processor for repeatedly retrieving a selected first word and a selected second word of the expanded key, at least one of which is retrieved from the memory, and generating from the selected first and second words a successive subsequent word of the expanded key;

means for providing the generated words of the expanded key to the cryptographic engine as round keys for performing subsequent cryptographic rounds;

means for storing successive ones of the generated subsequent words in the memory by cyclically overwriting previously generated words of the expanded key.

25. The apparatus of claim 24 further including control means for ensuring previously generated words are overwritten only after those words have been used as said first and/or said second selected words by the expansion processor.

26. The apparatus of claim 24 in which the number of word locations in memory is less than the number of words in the expanded key.

27. The apparatus of claim 24 in which the number of word locations in the memory is equal to Nk.

28. The apparatus of claim 27 in which the words of the initial key are also overwritten by words of the expanded key during the overwriting.

29. The apparatus of claim 24 in which the number of word locations in the memory is equal to 2Nk.

30. The apparatus of claim 24 in which the memory is divided into two parts, a first part storing the initial key and the second part receiving the successively generated words of the expanded key.

31. The apparatus of claim 30 in which the means for storing stores the final round key in the second part of the memory and retains the initial key in the first part of the memory after completion of generation of the expanded key.

32. The apparatus of claim 31 further including means for performing a repeat key expansion starting with the initial key stored in the first part of the memory.

33. The apparatus of claim 31 further including means for performing an inverse key expansion starting with the final round key stored in the second part of the memory.

34. The apparatus of any one of claims 24 to 27 further including means for completing generation of the expanded key such that the final round key is stored in the memory and the initial key has been overwritten.

35. The apparatus of claim 34 further including means for performing an inverse key expansion starting with the final round key stored in the memory in order to regenerate the initial key for a subsequent cryptographic operation.

36. The apparatus of claim 30 in which the number of word locations in memory is equal to 2Nk, the first and the second parts having Nk locations each.

37. The apparatus of any preceding claim in which the expansion processor includes means for generating successive words of the AES Rijndael block cipher round keys according to the AES key expansion function.

38. The apparatus of claim 37 in which Nk = 8.

39. The apparatus of any preceding claim in which the expansion processor generates words of encryption round keys.

40. The apparatus of any one of claims 24 to 38 in which the expansion key processor generates words of decryption round keys.

41. The apparatus of claim 24 further including a cryptographic engine, and means for providing the generated words of the expanded key to the cryptographic engine on a word-by-word basis as the cryptographic engine consumes the words as round keys.

42. The apparatus of claim 24 further including means for retrieving both the selected first word and the selected second word from the memory.

43. The apparatus of claim 24 further including means for retrieving the selected first word from memory and the selected second word from a register in the expansion processor.

44. The apparatus of claim 1 further including a cryptographic engine, in which the expansion processor and the cryptographic engine share an S-box.

45. The apparatus of claim 44 further including the means for maintaining synchronism of the expansion processor and the cryptographic engine.

46. A smart card incorporating the round key generator according to any one of claims 24 to 45.

47.A method of generating successive round key words of an expanded key, from an initial key, which method maintains the generated successive round key words in memory substantially only as long as they are required for use in the generation of successive round key words and for use in the parallel operation of a cryptographic process.

48. The method of claim 47 in which the initial key words are also maintained in the memory during the entire process of generating the expanded key.

49. An AES round constant function generator comprising a shift register having:

a first control input for causing a left shift of the register contents;

a second control input for causing a right shift of the register contents; and

a third control input for causing a preset of the shift register contents to one of several possible values.

50. The apparatus of claim 49 in which the third control input causes a preset of the shift register contents to a value that is determined according to the current contents of the register.

51. The apparatus of claim 49 in which the several possible values are 01, 1B, 36, 80 and 40 in hexadecimal.

52. The apparatus of claim 49 in which the first control input is asserted once for each round of an AES encryption operation, and in which the second control input is asserted once for each round of an AES decryption operation.

53. Apparatus substantially as described herein with reference to the accompanying drawings.

54. A method substantially as described herein with reference to the accompanying drawings.